

Appl. No. 09/536,577

Reply to Office Action of August 10, 2005

REMARKS

In the August 10, 2005 Office Action, claims 1, 3, 4, and 6-11 were allowed, and claims 12-15 were rejected. Applicant respectfully declines to amend the claims at this time. Reconsideration of the application is respectfully requested in view of the following remarks.

Claims 12-15 stand rejected under 35 U.S.C. §102(b) as being anticipated by Fiat, USPN 5,592,552 (hereinafter "Fiat"). Applicant traverses this rejection, which has been maintained throughout the prosecution of this application. Specifically, the Office Action states that:

The Broadcast Encryption method disclosed by Fiat includes a hierarchy of encryption keys, with keys assigned to nodes at each level (see column 12, line 58 to column 13, line 10). The nodes as shown by Fiat (see Figure 3) are organized in a balanced tree, and it is impossible to assign every node a unique set of $\log r$ keys unless keys are organized in a hierarchical manner. Each node *must* have one key corresponding to each tier of the hierarchy from the top of the tree to that node. Since the encryption device directly uses the memory, the devices must be coupled using electronic circuitry.

In response to Applicant's previous argument, the Office Action states: "Because Fiat discloses the presence of only $\log n$ keys with respect to a leaf, the usage and storing of tier-group specific key exchanging is inherent." Applicant disagrees with the above characterization of Fiat and, therefore, submits that Fiat does not teach or suggest each and every limitation recited in claims 12-15.

Fiat discloses a broadcast encryption technique that enables selective broadcasting of content to a restricted subset of users. The Fiat system is described in the context of a television broadcasting system, where only a defined subset of users/subscribers are allowed access to a given broadcast program. In order to achieve selective broadcasting, the Fiat system utilizes an encryption key technique. Fiat is directed to an encryption key distribution scheme that allows the broadcast system to identify a subset of users from among the entire population of users, where that subset is provided the encryption key (or keys) necessary for obtaining access to the securely broadcast program. In other words, authorized users can watch the program because

Appl. No. 09/536,577

Reply to Office Action of August 10, 2005

they have appropriate encryption keys, while unauthorized users are unable to watch the program because they do not have appropriate encryption keys. The Fiat system attempts to distribute the encryption keys to the users in an efficient manner that conserves bandwidth and system resources.

Fiat's FIG. 3 is simply a diagram that depicts the distribution paths of encryption keys to the subscribers. FIG. 3 represents a tree structure that allows any given subscriber (e.g., subscriber #5) to be removed from an authorized subset. Notably, Fiat's FIG. 3 does not represent a nodal structure wherein encryption keys are distributed at levels other than the ultimate subscriber level. In this regard, the "nodes" identified by letters A, B, C, D, E, F, and G are simply branches that are used to identify the subscriber paths. Encryption keys are only distributed to the subscribers, which are all resident at the same "level." See Fiat at column 5, lines 11-34 for a description of this tree structure.

Fiat neither teaches nor suggests the features or functions outlined in the above excerpt from the Office Action. For example, Fiat does not disclose "a hierarchy of encryption keys, with keys assigned to nodes at each level," and the cited passage of Fiat (column 12, line 58 to column 13, line 10) does not support this characterization of Fiat. Rather, this passage of Fiat describes how the total subscriber population is partitioned into subpopulations, and how each subpopulation includes *m* subscriber sets. In this context, a subscriber set is a group of users that either has authorized access to a secure program or a group of users that does not have authorized access to a secure program. This passage goes on to describe a technique for distributing encryption keys to the subscribers, using the conceptual tree structure as a tool for defining the distribution paths to the individual subscribers within the designated subscriber set. Again, and importantly, this passage does not teach or suggest encryption keys assigned to nodes at each level and, consequently, this passage does not teach or suggest a hierarchy of encryption keys.

In view of the above explanation of Fiat, the following passage from the Office Action is curious: "it is impossible to assign every node a unique set of $\log r$ keys unless keys are organized in a hierarchical manner. Each node *must* have one key corresponding to each tier of the hierarchy from the top of the tree to that node." Applicant has found no support for this

Appl. No. 09/536,577

Reply to Office Action of August 10, 2005

proposition in Fiat, and respectfully asks that the Examiner reconsider this characterization of Fiat. Furthermore, Applicant challenges the Examiner's conclusion that "the usage and storing of tier-group specific key exchanging is inherent" in Fiat due to the teaching of "log n keys with respect to a leaf." The term "log n keys" in Fiat simply refers to the number of different encryption keys needed to differentiate the subsets of subscribers for purposes of broadcasting secure programs. Thus, the statement regarding inherency seems to be misplaced in this context. If the Examiner decides to maintain this rejection, Applicant requests clarification on the above characterizations of Fiat, along with specific citations to those sections of Fiat that support the rejection.

Again, Fiat does not anticipate the invention of independent claim 12. In particular, Fiat does not teach or suggest a storage device that holds "a hierarchy of tier-group specific key encryption keys" as claimed. Rather, the Fiat system only utilizes a single "tier" of encryption keys – those distributed to the users/subscribers (as explicitly shown in FIG. 3 of Fiat). Applicant has discussed this shortcoming of Fiat extensively in the past, and respectfully refers the Examiner to the discussion of claims 12-15 set forth in the Response originally dated March 14, 2005, in the Response dated July 30, 2004, and in the Response dated March 30, 2004.

For at least the above reasons (and for the reasons set forth in Applicant's previous Responses), independent claim 12 is not anticipated by Fiat. For the same reasons, claims 13-15, which variously depend from claim 12, are also not anticipated by Fiat. Accordingly, claims 12-15 are allowable over Fiat and Applicant requests the withdrawal of the §102 rejection of claims 12-15.

In conclusion, for the reasons given above, all claims now presently in the application are believed allowable and such allowance is respectfully requested. Should the Examiner have any questions or wish to further discuss this application, Applicants request that the Examiner contact the undersigned attorney at (480) 385-5060.

If for some reason Applicants have not requested a sufficient extension and/or have not paid a sufficient fee for this response and/or for the extension necessary to prevent abandonment

Appl. No. 09/536,577

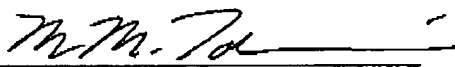
Reply to Office Action of August 10, 2005

on this application, please consider this as a request for an extension for the required time period and/or authorization to charge Deposit Account No. 50-2091 for any fee which may be due.

Respectfully submitted,

INGRASSIA FISHER & LORENZ

Dated: November 8, 2005

By: 
Mark M. Takahashi
Reg. No. 38,631
(480) 385-5060